平成１７年度研究ステーション研究成果報告書

1. 研究ステーション名・代表者名

研究ステーション名　情報理論基礎応用研究ステーション
代表者名　小林　欣吾

2. 平成１７年度の研究の特筆すべき成果

情報理論基礎応用研究ステーション提案の２つのプロジェクト、
1) 「情報理論の研究とネットワーク符号化への応用とその実証的実験」（代表者：小林欣吾）
2) 「公開鍵暗号の安全性に関する評価と計算機実験」（代表者：太田和夫）
のうち，1) はそれまでの「情報通信に関わる離散データの符号化の研究とその実証的実験」というプロジェクトを受け継いで，近年注目を浴びているネットワーク符号化を意識したテーマに力点を移しながら発展的に研究活動を広げてきているが，いずれも前年度に引き続き同一のオープンラボ室を利用して活動を実施してきている．これらのプロジェクトは，メンバー教員による，科学研究費補助金が交付された研究テーマ，民間との共同研究を円滑に推進するために有効に働いてきた．特に，セキュリティに関する研究グループでは，専用暗号解読ハードウェアによる暗号の安全性評価を行った．近年，ソフトウェア実装だけではなく，暗号解読を専用装置のデザインがいくつか提案されており，その真の影響を探ることは，急務となっている．我々の研究グループは，実現の可能性が高いと期待される YASD というデザインをターゲットに絞り，現在のデファクトスタンダードであり 1024 ビット RSA 暗号を解読するのに必要なコスト，年数を正確に評価した．その結果，直径 30cm の 1 つの wafer を用いた場合，約 1 万年程度の時間が必要であることを明らかにした．

3. 平成１７年度の研究成果の公表実績（主催した研究会、研究成果の発信状況等）

以下の研究セミナーを学術講演会, IS セミナー，研究室セミナーとして情報理論基礎応用研究ステーションが主催，共催などの形をとって行った．

1. 日時　：平成 17 年 4 月 14 日（木）16:00 18:00
   講演者： Paul H. Siegel (Professor, Department of Electrical and Computer Engineering, University of California, San Diego)
   題目： Constrained Coding Techniques for Advanced Data Storage Devices
2. 日時　：平成 17 年 10 月 4 日 (火) 9:00 〜 10:00
   講演者： Dr. Taraz, Anusch （ドイツ・ミュンヘン工科大学・数学科・教授）
   題目　：Large planar subgraphs in dense graphs
3. 日時　：平成 17 年 11 月 11 日（金）15:00〜17:00
   講演者： Prof. Marat Burnashev (Russian Academy of Sciences)
   題目　：On Some Singularities in Parameter Estimation Problems
4. 日時　：平成 18 年 3 月 17 日 (金) 15:30 〜 17:00
   講演者： 玉城史朗教授（琉球大学工学部）
   題目　：「閾値秘密分散法に基づくネットワークストレージ法に関する研究」

4. 外部資金の獲得状況

科学研究費補助金

基盤研究（B）	1 件	6,400,000 円
基盤研究（C）	8 件	8,500,000 円
特定領域研究 (2)	1 件	5,200,000 円
特別研究員奨励費	1 件	600,000 円
調査研究助成	2 件	1,800,000 円
共同研究	5 件	7,000,000 円
委託研究	3 件	4,100,000 円

5. 今後の研究発展（外部への発信、外部資金獲得計画を含む）

情報理論，情報セキュリティの研究分野で国際的に活躍している研究者を多数擁している我々のグループは，平成１５年度は IEEE 国際情報理論シンポジウム横浜のプログラム委員会の中核として活動し，また，文科省の国際シンポジウム支援経費を得て，第３回アジア・ヨーロッパ情報理論ワークショップを電通大の主催により千葉・鴨川において開催し，成功をおさめた．平成１６年度は海外からの一流の研究者６名を本学に招き８つの講演を開催した．平成１７年度は海外からの研究者３名，国内から１名を本学に招き４つの講演を開催した．これらの研究セミナーの開催案内は学外の連携する研究者グループに適切に伝えられ，電通大の大学院生，学部学生，教員に限らず，常に多数の学外研究者が参加してきた．このように開かれた研究セミナーを，本年度もこれまでどおり継続していく．

また，平成１７年度から，ステーションのメンバー教員の指導している博士後期課程の院生に，定期的に彼らの研究の発表の機会を与え，指導教員以外からの熟達した教員による批判と助言を得られるようにするという計画は関係する教員が多忙を極めたため実施に遅延が生じたが，平成１８年度には実施できるように準備を始めている．これが軌道にのれば，幅広い視野と深い洞察力で裏打ちされた，国際的な舞台でも直ちに活躍できる若手研究者の育成が可能となろう．なお，ステーションの主導による外部資金獲得計画はとくに立案せず，各研究者の自立的な努力により外部資金を増やしていくこととしていることは例年のとおりである．

なお，平成１６年度から UCSD から JSPS を通してポストドクの Dr.Kurkoski が我々のメンバーに加わり，院生はもとより，グループに研究上の好ましい刺激を引き続き与えてくれている．平成１８年２月には UCSD には情報理論とその応用研究センター（Center for Information Theory and Applications) が設立され，その記念すべき開所ワークショップが開催された．ここには，我々の多くのメンバーが招待されたが，卒研発表，修論発表の時期と重なったため，小林，Kurkoski だけがステーションメンバーとして参加した．CALIT2(California Institute for Telecommunication and Information Technology) の中心的大学として UCSD が位置しており，その理論的中核を形成するのがこのセンターである．開所ワークショップには世界から気鋭の研究者 500 名ほどが参加し，１週間にわたってパラレル３セッションで熱気のある研究発表が行われた．鴨川ワークショップ以来培って来た UCSD の研究者達と我々のステーション関係者との研究交流を加速したいと考えている．いずれにせよ，国際的にも評価される活動のためには思い切った資金の投入も必要なときがくるかもしれない．大学，民間の支援が得られることも期待したい．

6. 代表的なピアレビュー論文発表、学会プレナリ、招待講演発表、特許出願、受賞等

ピアレビュー論文発表

[1] Hajime Matsui, Syojiro Sakata, Msazumi Kurihara, Seiichi Mita, “Systolic array architecture implementing Berlekamp-Massey-Sakata algorithm for decoding codes on a class of algebraic curves,” IEEE Trans. on Information Theory, Vol.51, No.11, pp.3856-3871, 2005.

[2] Hajime Matsui, Shojiro Sakata and Masazumi Kurihara, “Fast parallel decoding on systolic array architecture for codes on an class of algebraic curves,” Kokyuroku, RIMS, Kyoto Univ., Vol. 1420 , pp.183 － 205, 2005.

[3] 木村, 大西, 小早川, 星, 大森,“任意の Lp 距離による検索を可能とす る距離変換規則,” 情報処理学会論文誌・データベース, Vol. 46, No. SIG 8(TOD26), pp. 93–105, 2005.

[4] Michihiro Kobayakawa, Mamoru Hoshi, and Kensuke Onishi, “A Method for retrieving music data with different bit rates using MPEG-4 TwinVQ Audio Compression,” Proc. of ACM Multimedia (MM2005), pp. 459–462, 2005.

[5] M. M. Rashid, T. Kawabata, “Theoretical Analysis of a Zero-redundancy Estimator with a Finite Window for a Markovian Source,” IEICE Transactions on Fundamentals, E88-A, pp.2819-2825, 2005.

[6] 長岡浩司,「量子情報幾何の世界」（招待論文）, 電子情報通信学会論文誌 vol.J88-A, No.8, pp.874-885, 2005.

[7] 青木真吾, 森田啓義, 荒俣吉壮, 西新幹彦, “マクロブロックタイプを用いた MPEG2 圧縮動画像のカット点検出,” 情報処理学会論文誌：コンピュータビジョンとイメージメディア vol. 46, no. SIG15, pp. 51-58, 2005.

[8] Shuji Kawasaki, Hiroyoshi Morita, “On optimal scale upper bound in wavelet-based estimation for hurst index of fractional Brownian motion,” Journal of Interdisciplinary Mathematics, vol. 8, no. 2, pp. 195-214, 2005.

[9] Ken-ichi Iwata, Yasutada Oohama, “Information-Spectrum Characterization of Broadcast Channel with General Source,” IEICE Trans. Fundamentals, E88-A, 10, pp.2808-2818, 2005.

[10] Ken-ichi Iwata, Yasutada Oohama, “Information-Spectrum Characterization of Multiple-Access Channels with Correlated Sources,” IEICE Trans. Fundamentals, E88-A, 11, pp. 3196-3202, 2005.

[11] Dongzhao Sun, Mikihiko Nishaira, Hiroyoshi Morita, “On Multiple Smoothed Transmission of MPEG Video Streams,” IEICE Trans. on Fundamentals of Electronics, Communications and Computer Sciences, vol.E88-A, no.10, pp.2844-2851, 2005.

[12] T. Fukuda, N. Kanayama and K. Komatsu, “Prime divisors of special values of theta functions in the ray class field of a certain quadratic field modulo 2^n,” to appear in Math. Proc. of Cambridge Philosophical Society.

[13] 大久保誠也, 西野哲朗, 太田和夫, 國廣昇, “Bulk 量子計算モデル上における Grover のアルゴリズムの繰り返し回数について，” 情報処理学会論文誌：数理モデル化と応用，Vol. 46，No. SIG17(TOM13)，pp. 10-19，2005.

[14] 大久保誠也, 西野哲朗, 太田和夫, 國廣昇, “物理的実現可能性に優れた量子探索アルゴリズム，” 情報処理学会論文誌，Vol. 46，No. 6，pp. 1416-1425，2005.

[15] Yasuhiro Takahashi and Noboru Kunihiro, “A Linear-size Quantum Circuit for Addition with no Ancillary Qubits,” Quantum Information and Computation, Vol.5 No.6, pp.440-448, 2005.

[16] Yasuhiro Takahashi and Noboru Kunihiro, “A quantum circuit for Shor’s factoring algorithm using 2n+2 qubits,” Quantum Information and Computation, Vol.6 No.2, pp.184-192, 2006.

[17] Hyun-Ho Kang, Brian Kurkoski, Young-Ran Park, Hye-Joo Lee, Sang-Uk Shin, Kazuhiko Yamaguchi, Kingo Kobayashi, “A Viable System for Tracing Illegal Users of Video,” Lecture Notes in Computer Science, Vol. 3917 (International Workshop, WISI 2006), pp. 156-158, Springer-Verlag, 2006.

[18] Hyunho Kang, Brian Kurkoski, Kazuhiko Yamaguchi, Kingo Kobayashi, “Tracing Illegal Users of Video : Reconsideration of Tree-Specific and Endbuyer-Specific Methods・ Accepted for publication in Lecture Notes in Computer Science, (4th Workshop on Internet Communications Security, WICS2006), Springer-Verlag, 2006.

[19] Brian Kurkoski, Paul Siegel, Jack Wolf, “Soft-output Detector for Partial-Response Channels Using Vector Quantization,” IEEE Transactions on Magnetics, vol. 41, no. 10, pp. 2989-2991, October 2005.

[20] Hyun-Ho Kang, Brian Kurkoski, Young-Ran Park, Hye-Joo Lee, Sang-Uk Shin, Kazuhiko Yamaguchi, Kingo Kobayashi, "Video Fingerprinting System using Wavelets and Error Correcting Codes," Lecture Notes in Computer Science, Vol. 3786, pp. 150-164, Springer-Verlag, 2005.

[21] Kiyoshi Ando, Kiyoshi, Atsushi Kaneko, Ken-ichi Kawarabayashi, "Vertices of degree 5 in a contraction critically 5-connected graph," Graphs Combin. 21, no. 1, 27–37, 2005.

[22] Kiyoshi Ando, "Trivially noncontractible edges in a contraction critically 5- connected graph," Discrete Math. 293, no. 1-3, 61–72, 2005.

[23] 正津宗幸, 栗原正純, 杉村立夫, "Reed-Solomon 符号の最尤復号に関する検討," IEICE Tech. Report, IT2005-54, Vol.105, No.311, pp.19-24, 2005.

[24] Masazumi Kurihara, "Decoding algorithm for Iterated codes correcting compund- errors," Electronics and Communications in Japan, Part 3, Vol.3. No.1, pp.60-72, 2006.

[25] 栗原正純, 楯岡孝道, "組合せネットワーク上のルーティング制御とその応用," IEICE Tech. Report, Vol.105 No.662, IT2005-131, pp.211-216, 2006.

招待講演発表

[1] H. Nagaoka, "Differential Geometrical Aspects of Quantum Estimation Theory", COE-Kakenhi workshop on Quantum Information Theory and Quantum Statistical Inference, Proc. pp.9-11, Tokyo, 2005.

[2] H. Nagaoka, "A Quantum/Complex Extension of Information Geometry", The 2nd International Symposium on Information Geometry and Its Applications, Proc. pp.177-180, Tokyo, 2005.

[3] Kiyoshi Ando, "Contractible edges in k-connected graphs," The China-Japan Joint Conference on Discrete Geometry, Combinatorics and Graph Theory, Nankai University (Tianjin, China) and Northwestern Polytechnical University (Xi'an, China), Nov. 18-24, 2005.

[4] T. Kawabata, "Text Compression Algorithms –An Approach from Probabilistic Modelling–," Tutorial workshop on game-theoretic probability and related topics, Mar. 2006.

他に（阪田，2 件，太田 1 件，國廣 2 件）など，

国際学会プロシーディングス（査読あり）

[1] Shojiro Sakata, , "Multiple-Sequence BM Algorithm can be Replaced by a Succession of Single-Sequence BM Algorithm," Proc. 2005 IEEE International Symposium on Information Theory, pp. 1967-1971, Adelaide, Australia, 2005.

[2] Masaya Fujisawa, Shojiro Sakata, , "A Class of Quasi-Cyclic Regular LDPC Codes from Cyclic Difference Families with Girth 8," Proc. 2005 IEEE International Symposium on Information Theory, pp. 2290-2294, Adelaide, Australia, 2005.

[3] Kansuke Onishi, Mamoru Hoshi, "Optimal region for binary search tree, rotation and polytope," Proc. of the 5th International Symposium on Operations Research and Its Applications, Lhasa, Tibet, China, 255 - 266, August 8-13, 2005.

[4] Motohiro Nakanishi, Michihiro Kobayakawa, Mamoru Hoshi, Tadashi Ohmori, "A Method for Extracting a Musical Unit to Phrase Music Data in the Compressed Domain of TwinVQ Audio Compression," Proc. of Int. Conf. on Multimedia and Expo (ICME2005), 2005.

[5] M. M. Rashid, T. Kawabata, "Theoretical Analysis of a Zero-redundancy Estimator with a Finite Window for Memoryless Source," IEEE ITSOC Information Theory Workshop on Coding and Complexity, pp.171-175, 2005.

[6] Tsutomu Kawabata and You Yanagisawa, "Redundancy of Symbol Decomposition Algorithms for Memoryless Source," Proceedings of 2005 IEEE International Symposium on Information Theory, pp.500-504, 2005.

[7] Jun-ichi Takeuchi, Andrew Barron, Tsutomu Kawabata, "Statistical Curvature and Stochastic Complexity, " Proceedings of the Second International Symposium on Information Geometry and its Applications, 2nd IGAIA, pp.29-36, 2005.

[8] N. Yapage and H. Nagaoka, "A Quantum Extension of Boltzmann Machine: An Information Geometrical Approach", Proc. of Erato conference on Quantum Information Science (EQIS) 2005, pp.204-205, Tokyo (2005).

[9] M. Arimura and H. Nagaoka, "An Extension of Asymptotically Sufficient Statistic Method for Pointwise Strong Universality," Proc. 2005 IEEE International Symposium on Information Theory, pp. 505-509, Adelaide, Australia, 2005.

[10] H. Morita, M. Satoh, and A. J. van Wijngaarden, "On Multimode Polarity-Switch Codes of Rate 1-1/n," Proc. 2005 IEEE International Symposium on Information Theory, pp. 387-391, Adelaide, Australia, 2005.

[11] Hiroyoshi Morita and Takahiro Ota, "A Tight Upper Bound on the Size of the Antidictionary of a Binary String," Proceedings of Analysis of Algorithms 2005, Barcelona, Spain, June 2005.

[12] Ken-ichi Iwata, "On Multiple-Access Communication System for General Correlated Sources with an Array of General Independent Channels," Proc. 2005 IEEE International Symposium on Information Theory, pp. 142-146, Adelaide, Australia, 2005.

[13] I Gusti Bagus Baskara Nugraha, Mikihiko Nishiara, Hiroyoshi Morita, "A Hybrid Multicast Communication System for Internet Video Broadcasting," International Symposium on Communicationsand Information Technologies, pp.190-193, 2005.

[14] M. Mambo, M. R. Salinas, K. Ohta and N. Kunihiro, "Problems on the MR Micropayment Schemes," in Proceedings of ASIACCS2006.

[15] Yuichiro Esaki, Noboru Kunihiro and Kazuo Ohta, "Untraceable Off-Line Verifiable Quantum Cash," in Proc. of TQC2006.

[16] Y. Hanatani, Yuichi Komano, Kazuo Ohta and Noboru Kunihiro, "Provably Secure Electronic Cash based on Blind Multisignature Schemes, " 10th Financial Cryptography and Data Security Conference (FC 06).

[17] Y. Komano, K. Ohta, A. Shimbo and S. Kawamura, "Toward the Fair Anonymous Signatures: Deniable Ring Signature," CT-RSA2006, pp. 174-191, 2006.

[18] Y. Naito, Y. Sasaki, N. Kunihiro and K. Ohta, "Improved Collision Attack on MD4 with Probability Almost 1," ICISC2005, 2005.

[19] Y. Komano, K. Ohta, A. Shimbo and S. Kawamura, "On the Security of Probabilistic Multisignature Schemes and their Optimality," MyCrypt2005, pp.132-150, 2005.

[20] Y. Takahashi and N. Kunihiro, "A linear-size quantum circuit for addition with no ancillary qubits," EQIS2005, pp.113-114, 2005.

[21] N. Kanayama, M. Kida, N. Kunihiro, T. Nishino, K. Ohta and S. Okubo, "Quantum Algorithms for Solving Exact Shortest Vector Problem," EQIS2005, pp.179-180, 2005.

[22] T. Izu and N. Kunihiro, K. Ohta and T. Shimoyama, "Analysis on the Clockwise Transposition Routing for Dedicated Factoring Devices," WISA2005, pp. 232-242, 2005.

[23] Brian Kurkoski, Kazuhiko Yamaguchi, "Turbo Equalization as a Post-Processor for Partial-Response Channels," to appear in Digests of the 2006 IEEE International Magnetics Conference.

[24] Hyun-Ho Kang, Brian Kurkoski, Young-Ran Park, Hye-Joo Lee, Sang-Uk Shin, Kazuhiko Yamaguchi, Kingo Kobayashi, "Video Fingerprinting System using Wavelets and Error Correcting Codes," in Proceedings of 6th International Workshop on Information Security Applications 2005 (WISA 2005), pp. 323-338.

[25] Brian Kurkoski, Kazuhiko Yamaguchi, Kingo Kobayashi, "On BCJR State Metric Quantization for Turbo Equalization," in Proceedings of the International Symposium on Information Theory, pp. 234-238, Sept. 2005.

[26] Brian Kurkoski, Paul Siegel, Jack Wolf, "Soft-output Detector for Partial-Response Channels Using Vector Quantization," in Digests of the IEEE International Magnetics Conference, p. 801, April 2005.

査読なし国際会議，国内発表

[1] 大西 建輔, 小早川 倫広, 木村 彰宏, 星 守, 大森 匡, "任意の Lp 距離関数による検索が可能な索引構造," 情報処理学会研究会報告 アルゴリズム研究会, AL-103, pp. 67–76, 2005.

[2] 山本 敦, 小早川 倫広, 星 守, 大森 匡, "画像の領域分割に基づく類似画像検索," 情報処理学会研究会報告オーディオビジュアル複合研究会，AVM-52, pp.19–26, 2006.

[3] Kamal Elkhaili, Tsutomu Kawabata, "Broadcasting for Dirty Printers," Proceedings of the 28th Symposium on Information Theory and Its Applications, Vol. 1, pp. 67-70, 2005.

[4] 太田隆博, 森田啓義, "Suffix tree を用いた反辞書の生成法について," 信学技報, July 2005.

[5] Takahiro Ota and Hiroyoshi Morita, "Linear Complexity Construction of Antidicitonaries," Proc. of the 28th Symposium on Information Theory and its Applications (SITA2005), Onna, Okinawa, pp.407–410, Nov. 2005.

[6] 太田隆博, 森田啓義, "反辞書木情報源モデルを用いたデータ圧縮," 信学技報， 名古屋，Mar. 2006.

[7] 渡邊大, 西新幹彦, 森田啓義, "算術符号における符号語の生成過程の確率モデルについて", 信学技報，名古屋，Mar. 2006.

[8] 島貫至行, ブライアン クルカスキー, 山口和彦, "Turbo-like 符号による低符号化率連接号の二、三の考察," 電子情報通信学会技術報告情報理論, 2006 年 3 月掲載予定.

[9] Hyunho Kang, Brian Kurkoski, Kazuhiko Yamaguchi, Kingo Kobayashi, "Tracing Illegal Users of Video Content: Reconsideration of Tree-Specific and Endbuyer Specific Methods," 電子情報通信学会 2006 年 暗号と情報セキュリティシンポジウム, 2006.

[10] Brian Kurkoski, Kazuhiko Yamaguchi, Kingo Kobayashi, "Turbo Decoding Based on the Lookup-Table Algorithm," 第 28 回情報理論とその応用シンボジウム予稿集 (Proceedings of the 28th Symposium on Information Theory and its Applications), pp. 503-506, 2005.

[11] 前原進也, ブライアン クルカスキー, 山口和彦, 小林欣吾, "Reed-Solomon 符号の硬判定復号を用いた連接符号のターボ復号の評価," 第 28 回情報理論とその応用シンボジウム予稿集 (Proceedings of the 28th Symposium on Information Theory and its Applications), pp. 351-354, 2005.

[12] Hyunho Kang, Brian Kurkoski, Kazuhiko Yamaguchi, Kingo Kobayashi, "Tracing Illegal Users of Video Content Using Watermarking and Fingerprinting," 第 28 回情報理論とその応用シンボジウム予稿集 (Proceedings of the 28th Symposium on Information Theory and its Applications), pp. 483-486, 2005.

[13] Brian Kurkoski, Kazuhiko Yamaguchi, "Vector Quantization of Convolutional Decoder State Metrics," in Proceedings of Hawaii, IEICE and SITA Joint Conference on Information Theory, 電子情報通信学会技術報告情報理論, IT2005-21, pp. 15-20, 2005.

[14] Masato Yabe, Kazuhiko Yamaguchi, Brian Kurkoski, Kingo Kobayashi, “A Decoding Algorithm for LDPC Codes using Threshold Control for the Burst Error Channel,” in Proceedings of Hawaii, IEICE and SITA Joint Conference on Information Theory, 電子情報通信学会技術報告情報理論, IT2005-21, pp. 121-124, 2005.

など多数

著書, 解説記事

[1] H. Nagaoka, Asymptotic Theory of Quantum Statistical Inference, (ed. M. Hayashi), World Scientific (2005).

[2] 太田和夫, 國廣昇,「ほんとうに安全？現代の暗号」, 岩波書店,2005 年 5 月.

[3] 阪田省二郎, 栗原正純, 松井一, 藤沢匡哉,「誤り訂正符号入門」, 森北出版株式会社, 2005.

[4] 國廣昇, 太田和夫,「暗号の米政府標準方式が危機に」, 岩波書店「科学」, 2005 年 11 月号, p.1235-1237.